Shima
Filed 9/26/03
Q77708
1 of 1

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１０月　２日

出願番号
Application Number: 特願２００２－２９０３８７

[ST. 10/C]: [ＪＰ２００２－２９０３８７]

出願人
Applicant(s): 日本電気株式会社

２００３年　８月　８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０６３９１９

【書類名】　特許願
【整理番号】　65700120
【提出日】　平成14年10月 2日
【あて先】　特許庁長官　殿
【国際特許分類】　G09C　1/00
　　H04L　9/00
【発明者】
　【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
　【氏名】　島　成佳
【特許出願人】
　【識別番号】　000004237
　【氏名又は名称】　日本電気株式会社
【代理人】
　【識別番号】　100102864
　【弁理士】
　【氏名又は名称】　工藤　実
【選任した代理人】
　【識別番号】　100099553
　【弁理士】
　【氏名又は名称】　大村　雅生
【手数料の表示】
　【予納台帳番号】　053213
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9715177
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子データ送受信システム

【特許請求の範囲】

【請求項１】　ネットワークに接続され、第１番目から第ｎ番目（ｎは２以上の整数）までのｎ個の装置と、

前記ネットワークに接続され、第１電子データを第１装置に送信する送信装置と、

前記ネットワークに接続され、第ｎ装置からの第（ｎ＋１）電子データを受信する受信装置とを具備し、

第ｊ装置（１≦ｊ≦ｎを満たす整数）は、自己を識別する署名を第ｊ電子データに付与した第（ｊ＋１）電子データを生成して第（ｊ＋１）装置に送信し、

前記ｊが前記ｎのとき、第（ｎ＋１）装置は前記受信装置に対応する

電子データ送受信システム。

【請求項２】　請求項１に記載の電子データ送受信システムにおいて、

前記送信装置は、前記第１電子データと前記第１電子データの送信を認証する送信者認証子とを前記第１装置に送信し、

前記第１装置は、前記第１電子データと前記送信者認証子とに前記第１装置の署名を付与した第２電子データを生成して第２装置に送信する

電子データ送受信システム。

【請求項３】　請求項２に記載の電子データ送受信システムにおいて、

更に、

送信装置用記憶装置を具備し、

前記第１装置は、前記第１電子データと前記送信者認証子とに前記第１装置の署名を付与した電子データである送信証拠データを生成して前記送信装置に送信し、

前記送信装置は、前記第１装置からの前記送信証拠データを前記送信装置用記憶装置に格納する

電子データ送受信システム。

【請求項４】　請求項２又は３に記載の電子データ送受信システムにおいて、

前記第ｎ装置は、第（ｎ－１）装置からの前記第ｎ電子データを受信したとき、第ｎ電子データ受信通知を前記受信装置に送信し、

前記受信装置は、前記第ｎ電子データ受信通知に応じて、前記第ｎ電子データの受信を認証する受信者認証子を前記第ｎ装置に送信し、

前記第ｎ装置は、前記第ｎ電子データと前記受信者認証子とに前記第ｎ装置の署名を付与した第（ｎ＋１）電子データを生成して前記受信装置に送信する

電子データ送受信システム。

【請求項５】　請求項４に記載の電子データ送受信システムにおいて、

更に、

受信装置用記憶装置を具備し、

前記受信装置は、前記第ｎ装置からの第（ｎ＋１）電子データを前記受信装置用記憶装置に格納する

電子データ送受信システム。

【請求項６】　請求項４又は５に記載の電子データ送受信システムにおいて、

前記受信装置は、

前記送信者認証子と前記ｎ個の装置の署名とが格納された受信装置用データベースを備え、

前記第（ｎ＋１）電子データに付与された前記第ｎ装置の署名を除いた前記第ｎ電子データと前記受信者認証子とを取出し、

前記第（ｎ＋１）電子データ及び前記第２電子データ以外の前記第（ｊ＋１）電子データに付与された署名を除いた前記第ｊ電子データを取出し、

前記第２電子データに付与された前記第１装置の署名を除いた前記第１電子データと前記送信者認証子とを取出し、

前記受信装置用データベースを参照して、前記送信装置が前記第１電子データを送信したことを認識する

電子データ送受信システム。

【請求項７】　請求項６に記載の電子データ送受信システムにおいて、

前記第１装置は、前記送信装置から前記送信者認証子を受信した時刻を表す第１タイムスタンプに前記第１装置の署名を更に付与した前記第２電子データを生

成し、

前記第ｎ装置は、前記受信装置から前記受信者認証子を受信した時刻を表す第２タイムスタンプに前記第ｎ装置の署名を更に付与した前記第（ｎ＋１）電子データを生成し、

前記受信装置は、

前記第（ｎ＋１）電子データに付与された前記第ｎ装置の署名を除いた前記第ｎ電子データと前記受信者認証子と前記第２タイムスタンプとを取出し、

前記第２電子データに付与された前記第１装置の署名を除いた前記第１電子データと前記受信者認証子と前記第１タイムスタンプとを取出す

電子データ送受信システム。

【請求項８】　請求項４～７のいずれか一項に記載の電子データ送受信システムにおいて、

前記第ｎ装置は、前記第ｎ電子データと前記受信者認証子とに前記第ｎ装置の署名を付与した電子データである受信証拠データを生成して前記送信装置に送信する

電子データ送受信システム。

【請求項９】　請求項８に記載の電子データ送受信システムにおいて、

前記送信装置は、

前記ｎ個の装置の署名と前記受信者認証子とが格納された送信装置用データベースを備え、

前記受信証拠データに付与された前記第ｎ装置の署名を除いた前記第ｎ電子データと前記受信者認証子とを取出し、

前記受信証拠データ及び前記第２電子データ以外の前記第（ｊ＋１）電子データに付与された署名を除いた前記第ｊ電子データを取出し、

前記第２電子データに付与された前記第１装置の署名を除いた前記第１電子データと前記送信者認証子とを取出し、

前記送信装置用データベースを参照して、前記第１電子データが前記受信装置に送信されたことを認識する

電子データ送受信システム。

【請求項１０】　請求項９に記載の電子データ送受信システムにおいて、

更に、

第１電子データ記憶装置を具備し、

前記送信装置は、

前記第１電子データを送信する前に、前記第１電子データ記憶装置に前記第１電子データを格納し、

前記第１電子データを取出したとき、前記第１電子データ記憶装置を参照して、前記第１電子データが改ざんされることなく前記受信装置に送信されたことを認識する

電子データ送受信システム。

【請求項１１】　請求項１０に記載の電子データ送受信システムにおいて、

前記第ｎ装置は、前記第ｎ電子データと前記受信者認証子とに前記第ｎ装置の署名を付与した電子データである受信証拠データを生成し、前記受信証拠データから前記第１電子データを削除した受信証拠データを前記送信装置に送信し、

前記送信装置は、前記第ｎ装置からの前記削除された受信証拠データに、前記第１電子データ記憶装置に格納された前記第１電子データを付加して前記受信証拠データを復元する

電子データ送受信システム。

【請求項１２】　請求項９又は１１に記載の電子データ送受信システムにおいて、

前記第１装置は、前記送信装置から前記送信者認証子を受信した時刻を表す第１タイムスタンプに前記第１装置の署名を更に付与した前記第２電子データを生成し、

前記第ｎ装置は、前記受信装置から前記受信者認証子を受信した時刻を表す第２タイムスタンプに前記第ｎ装置の署名を更に付与した前記受信証拠データを生成し、

前記送信装置は、

前記受信証拠データに付与された前記第ｎ装置の署名を除いた前記第ｎ電子データと前記受信者認証子と前記第２タイムスタンプとを取出し、

前記第２電子データに付与された前記第１装置の署名を除いた前記第１電子データと前記受信者認証子と前記第１タイムスタンプとを取出す

電子データ送受信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、電子データ送受信システムに関し、特に、送信装置から送信された電子データが受信装置に受信されたか否かを確認する電子データ送受信システムに関する。

【０００２】

【従来の技術】

電子データ、電子文を送信するシステムが知られている（例えば、特許文献１、特許文献２、特許文献３、特許文献４参照。）。

送信装置が中継機器を介して受信装置に電子データを送信するシステムでは、送信装置が受信装置に電子データを送信したとき、例えば、送信装置を利用する送信者は、送信装置が送信した電子データを受信装置が受信したか否かを確認するために、送信装置により中継機器と通信してログを収集する必要がある。送信装置が送信した電子データを受信装置が受信するまで保証するシステムが望まれる。

【０００３】

【特許文献１】

特開２０００－７８２３５号公報

【特許文献２】

特開２０００－１８３８６６号公報

【特許文献３】

特開２００２－７２８８号公報

【特許文献４】

特開２００２－１８３４９１号公報

【０００４】

【発明が解決しようとする課題】

本発明の目的は、送信装置が送信した電子データを受信装置が受信するまで保証する電子データ送受信システムを提供することにある。

本発明の他の目的は、電子データが受信装置に送信された経路を検証することができる電子データ送受信システムを提供することにある。

本発明の更に他の目的は、電子データの改ざんを検出できる電子データ送受信システムを提供することにある。

本発明の更に他の目的は、ハッカーを防止する電子データ送受信システムを提供することにある。

【０００５】

【課題を解決するための手段】

以下に、［発明の実施の形態］で使用する番号・符号を用いて、課題を解決するための手段を説明する。これらの番号・符号は、［特許請求の範囲］の記載と［発明の実施の形態］の記載との対応関係を明らかにするために付加されたものであるが、［特許請求の範囲］に記載されている発明の技術的範囲の解釈に用いてはならない。

【０００６】

本発明の電子データ送受信システムは、第１番目から第ｎ番目（ｎは２以上の整数）までのｎ個の装置［５－１～５－ｎ］と、送信装置［１］と、受信装置［２］とを具備する。ｎ個の装置［５－１～５－ｎ］と送信装置［１］と受信装置［２］とはネットワーク［１００］に接続されている。送信装置［１］は、第１電子データを第１装置［５－１］に送信する。受信装置［２］は、第ｎ装置［５－ｎ］からの第（ｎ＋１）電子データを受信する。第ｊ装置（$1 \leqq j \leqq n$を満たす整数）は、自己を識別する署名を第ｊ電子データに付与した第（ｊ＋１）電子データを生成して第（ｊ＋１）装置に送信する。ここで、ｊがｎのとき、第（ｎ＋１）装置は受信装置［２］に対応する。

電子データとしては、業者同士の業務に関する文書が記載された電子メールが例示され、その電子メールには画像が添付されている場合もある。また、電子データとしては、その業者同士の業務に関する電子データの他に、金融に関する電

子データ、民政に関する電子データが例示される。

本発明の電子データ送受信システムによれば、第（ｊ＋１）電子データが生成されるまでに付与された署名により、送信装置［１］を用いて第１電子データを送信した送信者が第１電子データを送信していないと否認（送信拒否）することができない。したがって、本発明の電子データ送受信システムは、送信装置［１］が送信した第１電子データを受信装置［２］が受信するまで保証する。

【０００７】

本発明の電子データ送受信システムにおいて、第ｊ装置が第１装置［５－１］である場合、送信装置［１］は、第１電子データと第１電子データの送信を認証する送信者認証子とを第１装置［５－１］に送信する。第１装置［５－１］は、第１電子データと送信者認証子とに第１装置［５－１］の署名を付与した第２電子データを生成して第２装置［５－２］に送信する。

本発明の電子データ送受信システムによれば、送信装置［１］の署名に対応する送信者認証子と、第（ｊ＋１）電子データが生成されるまでに付与された署名とにより、送信装置［１］を用いて第１電子データを送信した送信者が第１電子データを送信していないと否認（送信拒否）することができない。したがって、本発明の電子データ送受信システムは、送信装置［１］が送信した第１電子データを受信装置［２］が受信するまで保証する。

【０００８】

本発明の電子データ送受信システムは、更に、送信装置用記憶装置［３］を具備する。第１装置［５－１］は、第１電子データと送信者認証子とに第１装置［５－１］の署名を付与した電子データである送信証拠データを生成して送信装置［１］に送信する。送信装置［１］は、送信装置［１］は、第１装置［５－１］からの送信証拠データを送信装置用記憶装置［３］に格納する。

本発明の電子データ送受信システムによれば、第１装置［５－１］の署名を付与した送信証拠データを送信装置用記憶装置［３］に格納するため、送信装置［１］を用いて第１電子データを送信した送信者が第１電子データを送信していないと否認（送信拒否）することができない。

【０００９】

本発明の電子データ送受信システムにおいて、第ｊ装置が第ｎ装置［５－ｎ］である場合、第ｎ装置［５－ｎ］は、第（ｎ－１）装置からの第ｎ電子データを受信したとき、第ｎ電子データ受信通知を受信装置［２］に送信する。受信装置［２］は、第ｎ電子データ受信通知に応じて、第ｎ電子データの受信を認証する受信者認証子を第ｎ装置［５－ｎ］に送信する。第ｎ装置［５－ｎ］は、第ｎ電子データと受信者認証子とに第ｎ装置［５－ｎ］の署名を付与した第（ｎ＋１）電子データを生成して受信装置［２］に送信する。

本発明の電子データ送受信システムによれば、送信者認証子と、第（ｊ＋１）電子データが生成されるまでに付与された署名と、受信装置［２］の署名に対応する受信者認証子とにより、送信装置［１］を用いて第１電子データを送信した送信者が第１電子データを送信していないと否認（送信拒否）することができない。また、本発明の電子データ送受信システムによれば、受信装置［２］を利用する受信者が第１電子データを受取っていないと否認（受信拒否）することができない。したがって、本発明の電子データ送受信システムは、送信装置［１］が送信した第１電子データを受信装置［２］が受信するまで保証する。

【００１０】

本発明の電子データ送受信システムは、更に、受信装置用記憶装置［４］を具備する。受信装置［２］は、第ｎ装置［５－ｎ］からの第（ｎ＋１）電子データを受信装置用記憶装置［４］に格納する。

第（ｎ＋１）電子データは、送信者認証子と、ｎ個の装置［５－１～５－ｎ］の署名と、受信者認証子とが付与された第１電子データである。本発明の電子データ送受信システムによれば、第（ｎ＋１）電子データを受信装置用記憶装置［４］に格納するため、受信装置［２］を利用する受信者が第１電子データを受取っていないと否認（受信拒否）することができない。

【００１１】

本発明の電子データ送受信システムにおいて、受信装置［２］は、送信者認証子とｎ個の装置［５－１～５－ｎ］の署名とが格納された受信装置用データベース［１８］を備えている。受信装置［２］は、送信装置［１］が第１電子データを送信したことを検証する。受信装置［２］は、第（ｎ＋１）電子データに付与

された第ｎ装置［５－ｎ］の署名を除いた第ｎ電子データと受信者認証子とを取出す。受信装置［２］は、第（ｎ＋１）電子データ及び第２電子データ以外の第（ｊ＋１）電子データに付与された署名を除いた第ｊ電子データを取出す。受信装置［２］は、第２電子データに付与された第１装置［５－１］の署名を除いた第１電子データと送信者認証子とを取出す。受信装置［２］は、受信装置用データベース［１８］を参照して、送信装置［１］が第１電子データを送信したことを認識する。

このように、本発明の電子データ送受信システムによれば、受信装置［２］が第（ｎ＋１）電子データ、第ｎ電子データ、…、第２電子データ、第１電子データの順で正しく確認（検証）できた場合、第１電子データは、送信装置［１］によって送信されたことが保証される。また、本発明の電子データ送受信システムによれば、受信装置［２］は、署名の履歴として第１電子データが受信装置［２］に送信された経路（送信装置［１］、ｎ個の装置［５－１～５－ｎ］、受信装置［２］）を検証することができる。受信者は、第１電子データが送信された経路をオフラインで確認することができる。この受信装置［２］は、ｎ個の装置［５－１～５－ｎ］と通信してログを収集することなく、第１電子データが送信された経路をオフラインで確認することができる。このため、ｎ個の装置［５－１～５－ｎ］は、ログを格納する必要がなく、そのための記憶装置を必要としない。また、本発明の電子データ送受信システムは、受信装置［２］によって経路を把握するため、ハッカーの防止になる。

【００１２】

本発明の電子データ送受信システムにおいて、第１装置［５－１］は、送信装置［１］から送信者認証子を受信した時刻を表す第１タイムスタンプに第１装置［５－１］の署名を更に付与した第２電子データを生成する。第ｎ装置［５－ｎ］は、受信装置［２］から受信者認証子を受信した時刻を表す第２タイムスタンプに第ｎ装置［５－ｎ］の署名を更に付与した第（ｎ＋１）電子データを生成する。受信装置［２］は、第（ｎ＋１）電子データに付与された第ｎ装置［５－ｎ］の署名を除いた第ｎ電子データと受信者認証子と第２タイムスタンプとを取出す。受信装置［２］は、第２電子データに付与された第１装置［５－１］の署名

を除いた第１電子データと受信者認証子と第１タイムスタンプとを取出す。

【００１３】

本発明の電子データ送受信システムにおいて、第ｎ装置［５－ｎ］は、第ｎ電子データと受信者認証子とに第ｎ装置［５－ｎ］の署名を付与した電子データである受信証拠データを生成して送信装置［１］に送信する。

【００１４】

本発明の電子データ送受信システムにおいて、送信装置［１］は、ｎ個の装置［５－１～５－ｎ］の署名と受信者認証子とが格納された送信装置用データベース［１８］を備えている。送信装置［１］は、第ｎ装置［５－ｎ］からの受信証拠データにより、受信装置［２］が第１電子データを受信したことを検証する。送信装置［１］は、受信証拠データに付与された第ｎ装置［５－ｎ］の署名を除いた第ｎ電子データと受信者認証子とを取出す。送信装置［１］は、受信証拠データ及び第２電子データ以外の第（ｊ＋１）電子データに付与された署名を除いた第ｊ電子データを取出す。送信装置［１］は、第２電子データに付与された第１装置［５－１］の署名を除いた第１電子データと送信者認証子とを取出す。送信装置［１］は、送信装置用データベース［１８］を参照して、第１電子データが受信装置［２］に送信されたことを認識する。

このように、本発明の電子データ送受信システムによれば、送信装置［１］が受信証拠データ、第ｎ電子データ、…、第２電子データ、第１電子データの順で正しく確認（検証）できた場合、第１電子データは、受信装置［２］によって受信されたことが保証される。本発明の電子データ送受信システムによれば、送信装置［１］は、署名の履歴として第１電子データが受信装置［２］に送信された経路（送信装置［１］、ｎ個の装置［５－１～５－ｎ］、受信装置［２］）を検証することができる。送信者は、第１電子データが送信されてきた経路をオフラインで確認することができる。この送信装置［１］は、ｎ個の装置［５－１～５－ｎ］と通信してログを収集することなく、第１電子データが送信されてきた経路をオフラインで確認することができる。このため、ｎ個の装置［５－１～５－ｎ］は、ログを格納する必要がなく、そのための記憶装置を必要としない。また、本発明の電子データ送受信システムは、送信装置［１］によって経路を把握す

るため、ハッカーの防止になる。

【００１５】

本発明の電子データ送受信システムは、更に、第１電子データ記憶装置［３／１８］を具備する。第１電子データ記憶装置［３／１８］は、上記の送信装置用記憶装置［３］、又は、上記の受信装置用データベース［１８］である。送信装置［１］は、第１電子データを送信する前に、第１電子データ記憶装置［３／１８］に第１電子データを格納している。送信装置［１］は、第１電子データを取出したとき、第１電子データ記憶装置［３／１８］を参照して、第１電子データが改ざんされることなく受信装置［２］に送信されたことを認識する。

また、本発明の電子データ送受信システムによれば、送信装置［１］は、取出した第１電子データと第１電子データ記憶装置［３／１８］に格納されている第１電子データとを比較することで第１電子データの改ざんを検出できる。

【００１６】

本発明の電子データ送受信システムにおいて、第ｎ装置［５－ｎ］は、第ｎ電子データと受信者認証子とに第ｎ装置［５－ｎ］の署名を付与した電子データである受信証拠データを生成し、受信証拠データから第１電子データを削除した受信証拠データを送信装置［１］に送信する。送信装置［１］は、第ｎ装置［５－ｎ］からの第１電子データが削除された受信証拠データに、第１電子データ記憶装置［３／１８］に格納された第１電子データを付加して受信証拠データを復元する。

【００１７】

本発明の電子データ送受信システムにおいて、第１装置［５－１］は、送信装置［１］から送信者認証子を受信した時刻を表す第１タイムスタンプに第１装置［５－１］の署名を更に付与した第２電子データを生成する。第ｎ装置［５－ｎ］は、受信装置［２］から受信者認証子を受信した時刻を表す第２タイムスタンプに第ｎ装置［５－ｎ］の署名を更に付与した受信証拠データを生成する。送信装置［１］は、受信証拠データに付与された第ｎ装置［５－ｎ］の署名を除いた第ｎ電子データと受信者認証子と第２タイムスタンプとを取出す。送信装置［１］は、第２電子データに付与された第１装置［５－１］の署名を除いた第１電子

データと受信者認証子と第１タイムスタンプとを取出す。

【００１８】

【発明の実施の形態】

添付図面を参照して、本発明による電子データ送受信システムの実施の形態を以下に説明する。

【００１９】

図１は、本発明の電子データ送受信システムの構成を示す。本発明の電子データ送受信システムは、送受信装置１、２と、記憶装置３と、記憶装置４と、第１番目から第ｎ番目（ｎは２以上の整数）までのｎ個の装置５－１～５－ｎとを具備する。送受信装置１、２と第１装置５－１、第２装置５－２、第３装置５－３、第４装置５－４、…、第ｎ装置５－ｎとはネットワーク１００に接続されている。送受信装置１には、送受信装置１用の記憶装置として記憶装置３が接続されている。送受信装置２には、送受信装置２用の記憶装置として記憶装置４が接続されている。

【００２０】

この本発明の電子データ送受信システムは、送受信装置１が送信した電子データを送受信装置２が受信するまで保証するものである。図２は、本発明の電子データ送受信システムの概念を示す。ここで、本発明の電子データ送受信システムを具体的に説明するために、ｎを５とし、第１装置５－１を受付機器５－１とし、第２装置５－２を中継機器５－２とし、第３装置５－３を中継機器５－３とし、第４装置５－４を中継機器５－４とし、第ｎ装置５－ｎを受付機器５－５とする。送受信装置１は、電子データを送受信装置２に送信するものとする。電子データは、送受信装置１から出力されて受付機器５－１、中継機器５－２、中継機器５－３、中継機器５－４、受付機器５－５を介して送受信装置２に出力される。

【００２１】

電子データとしては、業者同士の業務に関する文書が記載された電子メールが例示され、その電子メールには画像が添付されている場合もある。また、電子データとしては、その業者同士の業務に関する電子データの他に、金融に関する電

子データ、民政に関する電子データが例示される。ここで、電子データは文書が記載された電子データ（電子メール）とし、以下、その電子データを電子文書と称する。

【００２２】

図３は、送受信装置１、２の構成を示す。送受信装置１、２は、パーソナルコンピュータ、ワークステーション等で例示される情報処理装置である。送受信装置１、２は、コンピュータプログラムである送信部１１、受信部１２、署名部１３、署名検証部１４、電子文書検証部１５、電子文書作成部１６、登録部１７を備え、データベース１８を有する。送受信装置１、２には、利用者の操作により電子文書作成部１６が電子文書を作成するための入力装置（図示しない）が接続されている。送受信装置１、２の署名部１３は、公開鍵基盤を利用して秘密鍵で電子文書に送受信装置１、２の署名を行うものである。送受信装置１のデータベース１８には、受付機器５－１、５－５の署名、中継機器５－２、５－３、５－４の署名、送受信装置２の署名（後述の認証子）がそれぞれ公開鍵証明書として格納されている。送受信装置２のデータベース１８には、送受信装置１の署名（後述の認証子）、受付機器５－１、５－５の署名、中継機器５－２、５－３、５－４の署名がそれぞれ公開鍵証明書として格納されている。

【００２３】

図４は、受付機器５－１、５－５の構成を示す。受付機器５－１、５－５は、ワークステーション、サーバ等で例示される情報処理装置である。受付機器５－１、５－５は、コンピュータプログラムである送信部２１、受信部２２、署名部２３、署名検証部２４、証拠データ生成部２５、タイムスタンプ生成部２６、保存制御部２７を備え、データベース２８を有する。受付機器５－１のデータベース２８には、送受信装置１、２の署名（後述の認証子）、中継機器５－２、５－３、５－４の署名、受付機器５－５の署名がそれぞれ公開鍵証明書として格納されている。受付機器５－５のデータベース２８には、送受信装置１、２の署名（後述の認証子）、受付機器５－１の署名、中継機器５－２、５－３、５－４の署名がそれぞれ公開鍵証明書として格納されている。また、受付機器５－１、５－５の署名検証部２４は、送受信装置１、２のアドレスを予めに認識している。な

お、受付機器５－１、５－５をなくして、受付機器５－１、５－５の機能（送信部２１、受信部２２、証拠データ生成部２５、タイムスタンプ生成部２６、署名部２３、署名検証部２４、保存制御部２７、データベース２８）をアプリケーションとして送受信装置１、２に実装することも可能である。

【００２４】

図５は、中継機器５－２、５－３、５－４の構成を示す。中継機器５－２、５－３、５－４は、コンピュータプログラムである送信部３１、受信部３２、署名部３３、署名検証部３４を備え、データベース３８を有する。中継機器５－２のデータベース３８には、受付機器５－１、５－５、中継機器５－３、５－４の署名がそれぞれ公開鍵証明書として格納されている。中継機器５－３のデータベース３８には、受付機器５－１、５－５、中継機器５－２、５－４の署名がそれぞれ公開鍵証明書として格納されている。中継機器５－４のデータベース３８には、受付機器５－１、５－５、中継機器５－２、５－３の署名がそれぞれ公開鍵証明書として格納されている。本実施例では中継機器を３つとしている。しかし受付機器５－１、５－５同士が直接通信できる環境では中継機器５－２、５－３、５－４は必要ない。また電子文書の処理手続きのプロセスなどが長いときには中継機器が複数台存在する。

【００２５】

記憶装置３、記憶装置４は、フレキシブルディスク、ハードディスク、データベース、ファイルサーバ等で例示される装置である。記憶装置３、記憶装置４には、電子文書等で例示されるデータ（後述）が送受信装置１、２によって格納される。

【００２６】

次に、本発明の電子データ送受信システムの動作について説明する。

送受信装置１から出力される第１電子文書は、受付機器５－１、中継機器５－２、中継機器５－３、中継機器５－４、受付機器５－５を介して送受信装置２に出力される。このため、本発明の電子データ送受信システムの動作の説明では、送受信装置１を送信装置１とし、送受信装置２を受信装置２とする。

【００２７】

まず、第１電子文書の送受信の証拠となる署名データ（署名、送信認証子、送信証拠データ、受信認証子、受信証拠データ）の生成について説明する。

【００２８】

図６に示されるように、送信装置１を利用する送信者は、受信装置２に送る第１電子文書を作成するために、送信装置１の入力装置を操作する。送信装置１の電子文書作成部１６は、その入力装置の操作に応じて、第１電子文書を作成する（ステップＡ１）。

送信者が送信装置１の入力装置を操作して第１電子文書を受信装置２に送るとき、送信装置１の送信部１１は、その入力装置の操作に応じて、第１電子文書の送信要求を受付機器５－１に送信する（ステップＡ２）。

【００２９】

受付機器５－１の受信部２２は、送信装置１からの第１電子文書の送信要求を受信する。その受信部２２が第１電子文書の送信要求を受信したとき、受付機器５－１の署名部２３は、ランダムな文字列を生成する。受付機器５－１の送信部２１は、そのランダムな文字列を送信装置１に送信する（ステップＡ３）。

【００３０】

送信装置１の受信部１２は、受付機器５－１からのランダムな文字列を受信する。送信装置１の署名部１３は、その受信部１２が受信したランダムな文字列に送信装置１の秘密鍵で署名して、第１電子文書の送信を認証する送信者認証子を生成する（ステップＡ４）。

送信装置１の登録部１７は、送信装置１の送信部１１が第１電子文書を送信する前に、記憶装置３又は送信装置１のデータベース１８に第１電子文書を保管用電子文書として格納しておく（ステップＡ５）。ここで、この保管用電子文書は記憶装置３に格納されるものとする。

送信装置１の送信部１１は、第１電子文書と送信者認証子とを受付機器５－１に送信する（ステップＡ６）。ここで、第１電子文書は、第１電子文書を受信装置２宛てに送るためのアドレス（受信装置２のアドレス）を含む。

【００３１】

受付機器５－１の受信部２２は、送信装置１からの第１電子文書と送信者認証

子とを受信する。その受信部２２が第１電子文書と送信者認証子とを受信したとき、受付機器５－１のタイムスタンプ生成部２６は、送信装置１から送信者認証子を受信した時刻を表す第１タイムスタンプを生成する（ステップＡ７）。

このとき、受付機器５－１の署名検証部２４は、受付機器５－１のデータベース２８を参照して、送信者認証子と送信装置１の公開鍵証明書とを照合し、送信者認証子が送信装置１の公開鍵証明書と一致するか否かを検証する（ステップＡ８）。

【００３２】

検証の結果、一致する場合、受付機器５－１の証拠データ生成部２５は、第１電子文書に送信者認証子、第１タイムスタンプを加えてハッシュ値を生成する。受付機器５－１の証拠データ生成部２５は、そのハッシュ値に受付機器５－１の秘密鍵で署名することにより、第１電子文書と送信者認証子と第１タイムスタンプとに受付機器５－１の署名を付与した電子データである送信証拠データを生成する（ステップＡ９）。送信証拠データを生成する場合、第１タイムスタンプは省略してもよい。受付機器５－１の送信部２１は、送信証拠データを送信装置１に送信する（ステップＡ１０）。

また、検証の結果、一致しない場合、受付機器５－１の送信部２１は、一致しない旨を表す情報を送信装置１に送信する。送信装置１は、その情報に応じて、再度、第１電子文書と送信者認証子とを受付機器５－１に送信し、受付機器５－１は、再度、送信者認証子を検証しても一致しない場合、第１電子文書を送信できない旨を表す情報を送信装置１に送信する（このステップは図示しない）。

【００３３】

送信装置１の受信部１２は、受付機器５－１からの送信証拠データを受信する。その受信部１２が送信証拠データを受信したとき、送信装置１の署名検証部１４は、送信装置１のデータベース１８を参照して、送信証拠データの署名と受付機器５－１の公開鍵証明書とを照合し、送信証拠データの署名が受付機器５－１の公開鍵証明書と一致するか否かを検証する（ステップＡ１１）。

検証の結果、一致する場合、送信装置１の登録部１７は、送信証拠データを記憶装置３に格納する（ステップＡ１２）。本発明の電子データ送受信システムに

よれば、受付機器５－１の署名を付与した送信証拠データを記憶装置３に格納するため、送信装置１を用いて第１電子文書を送信した送信者が第１電子文書を送信していないと否認（送信拒否）することができない。

また、検証の結果、一致しない場合、送信装置１は、再度、第１電子文書と送信者認証子とを送信し、受付機器５－１は、再度、送信者認証子を検証しても一致しない場合、第１電子文書を送信できない旨を表す情報を送信装置１に送信する（このステップは図示しない）。

【００３４】

受付機器５－１の署名部２３は、第１電子文書に送信者認証子、第１タイムスタンプを加えてハッシュ値を生成する。受付機器５－１の証拠データ生成部２５は、そのハッシュ値に受付機器５－１の秘密鍵で署名することにより、第１電子文書と送信者認証子と第１タイムスタンプとに受付機器５－１の署名を付与した第２電子文書を生成する（ステップＡ１３、図９参照）。第２電子文書を生成する場合、第１タイムスタンプは省略してもよい。

受付機器５－１の送信部２１は、第２電子文書を中継機器５－２に送信する（ステップＡ１４）。第２電子文書は、受信装置２のアドレスを含む。

【００３５】

図７に示されるように、中継機器５－２の受信部３２は、受付機器５－１からの第２電子文書を受信する。その受信部３２が第２電子文書を受信したとき、中継機器５－２の署名検証部３４は、中継機器５－２のデータベース３８を参照して、第２電子文書の署名と受付機器５－１の公開鍵証明書とを照合し、第２電子文書の署名が受付機器５－１の公開鍵証明書と一致するか否かを検証する（ステップＡ１５）。その署名検証部３４は、検証することにより、中継してよいかどうかの正当性確認をする。ただし受付機器５－１と中継機器５－２の間に信頼関係が成立する場合は署名検証を省略してもよい。

【００３６】

検証の結果、一致する場合、中継機器５－２の署名部３３は、第２電子文書に中継機器５－２の秘密鍵で署名することによって、第２電子文書に中継機器５－２の署名を付与した第３電子文書を生成する（ステップＡ１６、図９参照）。中

継機器５－２の送信部３１は、第３電子文書を中継機器５－３に送信する（ステップＡ１７）。第３電子文書は、受信装置２のアドレスを含む。

また、検証の結果、一致しない場合、中継機器５－２の送信部３１は、一致しない旨を表す情報を受付機器５－１に送信する。受付機器５－１は、その情報に応じて、再度、第２電子文書を中継機器５－２に送信し、中継機器５－２は、再度、第２電子文書を検証しても一致しない場合、第２電子文書（第１電子文書）を送信できない旨を表す情報を送信装置１に送信する（このステップは図示しない）。

【００３７】

中継機器５－３の受信部３２は、中継機器５－２からの第３電子文書を受信する。その受信部３２が第３電子文書を受信したとき、中継機器５－３の署名検証部３４は、中継機器５－３のデータベース３８を参照して、第３電子文書の署名と中継機器５－２の公開鍵証明書とを照合し、第３電子文書の署名が中継機器５－２の公開鍵証明書と一致するか否かを検証する（ステップＡ１８）。その署名検証部３４は、検証することにより、中継してよいかどうかの正当性確認をする。ただし受付機器５－２と中継機器５－３の間に信頼関係が成立する場合は署名検証を省略してもよい。

【００３８】

検証の結果、一致する場合、中継機器５－３の署名部３３は、第３電子文書に中継機器５－３の秘密鍵で署名することによって、第３電子文書に中継機器５－３の署名を付与した第４電子文書を生成する（ステップＡ１９、図９参照）。中継機器５－３の送信部３１は、第４電子文書を中継機器５－４に送信する（ステップＡ２０）。第４電子文書は、受信装置２のアドレスを含む。

また、検証の結果、一致しない場合、中継機器５－３の送信部３１は、一致しない旨を表す情報を中継機器５－２に送信する。中継機器５－２は、その情報に応じて、再度、第３電子文書を中継機器５－３に送信し、中継機器５－３は、再度、第３電子文書を検証しても一致しない場合、第３電子文書（第１電子文書）を送信できない旨を表す情報を送信装置１に送信する（このステップは図示しない）。

【００３９】

中継機器５－４の受信部３２は、中継機器５－３からの第４電子文書を受信する。その受信部３２が第４電子文書を受信したとき、中継機器５－４の署名検証部３４は、中継機器５－４のデータベース３８を参照して、第４電子文書の署名と中継機器５－３の公開鍵証明書とを照合し、第４電子文書の署名が中継機器５－３の公開鍵証明書と一致するか否かを検証する（ステップＡ２１）。その署名検証部３４は、検証することにより、中継してよいかどうかの正当性確認をする。ただし受付機器５－３と中継機器５－４の間に信頼関係が成立する場合は署名検証を省略してもよい。

【００４０】

検証の結果、一致する場合、中継機器５－４の署名部３３は、第４電子文書に中継機器５－４の秘密鍵で署名することによって、第４電子文書に中継機器５－４の署名を付与した第５電子文書を生成する（ステップＡ２２、図９参照）。中継機器５－４の送信部３１は、第５電子文書を受付機器５－５に送信する（ステップＡ２３）。第５電子文書は、受信装置２のアドレスを含む。

また、検証の結果、一致しない場合、中継機器５－４の送信部３１は、一致しない旨を表す情報を中継機器５－３に送信する。中継機器５－３は、その情報に応じて、再度、第４電子文書を中継機器５－４に送信し、中継機器５－４は、再度、第４電子文書を検証しても一致しない場合、第４電子文書（第１電子文書）を送信できない旨を表す情報を送信装置１に送信する（このステップは図示しない）。

【００４１】

図８に示されるように、受付機器５－５の受信部２２は、中継機器５－４からの第５電子文書を受信する。その受信部２２が第５電子文書を受信したとき、受付機器５－５の署名検証部２４は、受付機器５－５のデータベース２８を参照して、第５電子文書の署名と中継機器５－４の公開鍵証明書とを照合し、第５電子文書の署名が中継機器５－４の公開鍵証明書と一致するか否かを検証する。その署名検証部２４は、受付機器５－５のデータベース２８を参照して、第５電子文書に含まれるアドレスにより受信装置２宛ての電子文書であるか否か確認する（

ステップＡ２４）。

【００４２】

検証と確認の結果、一致する場合、受付機器５－５の送信部２１は、第５電子文書を受信したことを表す受信通知を受信装置２に送信する（ステップＡ２５）。

また、検証の結果、一致しない場合、受付機器５－５の送信部２１は、一致しない旨を表す情報を中継機器５－４に送信する。中継機器５－４は、その情報に応じて、再度、第５電子文書を受付機器５－５に送信し、受付機器５－５は、再度、第５電子文書を検証しても一致しない場合、第５電子文書（第１電子文書）を送信できない旨を表す情報を送信装置１に送信する（このステップは図示しない）。

【００４３】

受信装置２の受信部１２は、受付機器５－５からの受信通知を受信する。その受信部１２が受信通知を受信したとき、受信装置２の送信部１１は、第５電子文書の受信要求を受付機器５－５に送信する（ステップＡ２６）。

【００４４】

受付機器５－５の受信部２２は、受信装置２からの第５電子文書の受信要求を受信する。その受信部２２が第５電子文書の受信要求を受信したとき、受付機器５－５の署名部２３は、ランダムな文字列を生成する。受付機器５－５の送信部２１は、そのランダムな文字列を受信装置２に送信する（ステップＡ２７）。

【００４５】

受信装置２の受信部１２は、受付機器５－５からのランダムな文字列を受信する。受信装置２の署名部１３は、その受信部１２が受信したランダムな文字列に受信装置２の秘密鍵で署名して、第５電子文書の受信を認証する受信者認証子を生成する（ステップＡ２８）。

受信装置２の送信部１１は、受信者認証子を受付機器５－５に送信する（ステップＡ２９）。

【００４６】

受付機器５－５の受信部２２は、受信装置２からの受信者認証子を受信する。

その受信部２２が受信者認証子を受信したとき、受付機器５－５のタイムスタンプ生成部２６は、受信装置２から受信者認証子を受信した時刻を表す第２タイムスタンプを生成する（ステップＡ３０）。

このとき、受付機器５－５の署名検証部２４は、受付機器５－５のデータベース２８を参照して、受信者認証子と受信装置２の公開鍵証明書とを照合し、受信者認証子が受信装置２の公開鍵証明書と一致するか否かを検証する（ステップＡ３１）。

【００４７】

検証の結果、一致する場合、受付機器５－５の署名部２３は、第５電子文書に受信者認証子、第２タイムスタンプを加えてハッシュ値を生成する。受付機器５－５の署名部２３は、そのハッシュ値に受付機器５－５の秘密鍵で署名することにより、第５電子文書と受信者認証子と第２タイムスタンプとに受付機器５－５の署名を付与した第６電子文書を生成する（ステップＡ３２、図９参照）。第６電子文書を生成する場合、第２タイムスタンプは省略してもよい。受付機器５－５の送信部２１は、第６電子文書を受信装置２に送信する（ステップＡ３３）。

また、検証の結果、一致しない場合、受付機器５－５の送信部２１は、一致しない旨を表す情報を受信装置２に送信する。受信装置２は、その情報に応じて、再度、受信者認証子を受付機器５－５に送信し、受付機器５－５は、再度、受信者認証子を検証しても一致しない場合、第５電子文書（第１電子文書）を送信できない旨を表す情報を送信装置１に送信する（このステップは図示しない）。

【００４８】

受信装置２の受信部１２は、受付機器５－５からの第６電子文書を受信する。その受信部１２が第６電子文書を受信したとき、受信装置２の署名検証部１４は、受信装置２のデータベース１８を参照して、第６電子文書の署名と受付機器５－５の公開鍵証明書とを照合し、第６電子文書の署名が受付機器５－５の公開鍵証明書と一致するか否かを検証する（ステップＡ３４）。

検証の結果、一致する場合、受信装置２の登録部１７は、第６電子文書を記憶装置４に格納する（ステップＡ３５）。第６電子文書は、送信者認証子と、署名（受付機器５－１、中継器５－２、中継器５－３、中継器５－４、受付機器５－

５）と、受信者認証子とが付与された第１電子文書である。本発明の電子データ送受信システムによれば、第６電子文書を記憶装置４に格納するため、受信装置２を利用する受信者が第１電子文書を受取っていないと否認（受信拒否）することができない。

また、検証の結果、一致しない場合、受信装置２の送信部１１は、一致しない旨を表す情報を受付機器５－５に送信する。受付機器５－５は、その情報に応じて、再度、第６電子文書を受信装置２に送信し、受信装置２は、再度、第６電子文書を検証しても一致しない場合、第６電子文書（第１電子文書）を送信できない旨を表す情報を送信装置１に送信する（このステップは図示しない）。

【００４９】

受付機器５－５の証拠データ生成部２５は、第５電子文書に受信者認証子、第２タイムスタンプを加えてハッシュ値を生成する。受付機器５－５の証拠データ生成部２５は、そのハッシュ値に受付機器５－５の秘密鍵で署名することにより、第５電子文書と受信者認証子と第２タイムスタンプとに受付機器５－５の署名を付与した電子データである受信証拠データを生成する（ステップＡ３６、図１０参照）。受信証拠データを生成する場合、第２タイムスタンプは省略してもよい。

受付機器５－５の送信部２１は、受信証拠データを送信装置１に送信する（ステップＡ３７）。受信証拠データは、受付機器５－５から中継機器５－４、中継機器５－３、中継機器５－２、受付機器５－１を介して送信装置１に送信される。または、受信証拠データは、受付機器５－５から直接、送信装置１に送信される。

【００５０】

送信装置１の受信部１２は、受付機器５－５からの受信証拠データを受信する。その受信部１２が受信証拠データを受信したとき、送信装置１の署名検証部１４は、送信装置１のデータベース１８を参照して、受信証拠データの署名と受付機器５－５の公開鍵証明書とを照合し、受信証拠データの署名が受付機器５－５の公開鍵証明書と一致するか否かを検証する（ステップＡ３８）。

【００５１】

検証の結果、一致する場合、送信装置１の登録部１７は、受信証拠データを記憶装置３に格納する（ステップＡ３９）。

また、検証の結果、一致しない場合、受信装置２の送信部１１は、一致しない旨を表す情報を受付機器５－５に送信する。受付機器５－５は、その情報に応じて、再度、受信証拠データを受信装置２に送信し、受信装置２は、再度、受信証拠データを検証しても一致しない場合、第６電子文書（第１電子文書）を受信しても受け付けない旨を表す情報を送信装置１に送信する（このステップは図示しない）。

【００５２】

本発明の電子データ送受信システムによれば、送信者認証子と、第６電子文書が生成されるまでに付与された署名（受付機器５－１、中継器５－２、中継器５－３、中継器５－４、受付機器５－５）と、受信者認証子とにより、送信装置１を用いて第１電子文書を送信した送信者が第１電子文書を送信していないと否認（送信拒否）することができない。また、本発明の電子データ送受信システムによれば、受信装置２を利用する受信者が第１電子文書を受取っていないと否認（受信拒否）することができない。したがって、本発明の電子データ送受信システムは、送信装置１が送信した第１電子文書を受信装置２が受信するまで保証する。

【００５３】

次に、受信装置２が行う第６電子文書の検証について説明する。

【００５４】

図１１に示されるように、受信装置２の電子文書検証部１５は、受信装置２のデータベース１８を参照して、記憶装置４に格納された第６電子文書の署名と受付機器５－５の公開鍵証明書とを照合し、第６電子文書の署名が受付機器５－５の公開鍵証明書と一致するか否かを検証する（ステップＢ１）。

検証の結果、受信装置２の電子文書検証部１５は、一致する第６電子文書に付与された受付機器５－５の署名を除いた第５電子文書と受信者認証子と第２タイムスタンプとを取出す（ステップＢ２、図９参照）。

【００５５】

受信装置２の電子文書検証部１５は、受信装置２のデータベース１８を参照して、第５電子文書の署名と中継機器５－４の公開鍵証明書とを照合し、第５電子文書の署名が中継機器５－４の公開鍵証明書と一致するか否かを検証する（ステップＢ３）。

検証の結果、受信装置２の電子文書検証部１５は、一致する第５電子文書に付与された中継機器５－４の署名を除いた第４電子文書を取出す（ステップＢ４、図９参照）。

【００５６】

受信装置２の電子文書検証部１５は、受信装置２のデータベース１８を参照して、第４電子文書の署名と中継機器５－３の公開鍵証明書とを照合し、第４電子文書の署名が中継機器５－３の公開鍵証明書と一致するか否かを検証する（ステップＢ５）。

検証の結果、一致するため、受信装置２の電子文書検証部１５は、第４電子文書に付与された中継機器５－３の署名を除いた第３電子文書を取出す（ステップＢ６、図９参照）。

【００５７】

受信装置２の電子文書検証部１５は、受信装置２のデータベース１８を参照して、第３電子文書の署名と中継機器５－２の公開鍵証明書とを照合し、第３電子文書の署名が中継機器５－２の公開鍵証明書と一致するか否かを検証する（ステップＢ７）。

検証の結果、一致するため、受信装置２の電子文書検証部１５は、第３電子文書に付与された中継機器５－２の署名を除いた第２電子文書を取出す（ステップＢ８、図９参照）。

【００５８】

受信装置２の電子文書検証部１５は、受信装置２のデータベース１８を参照して、第２電子文書の署名と受付機器５－１の公開鍵証明書とを照合し、第２電子文書の署名が受付機器５－１の公開鍵証明書と一致するか否かを検証する（ステップＢ９）。

検証の結果、一致するため、受信装置２の電子文書検証部１５は、第２電子文

書に付与された受付機器５－１の署名を除いた第１電子文書と送信者認証子と第１タイムスタンプとを取出す（ステップＢ１０、図９参照）。

【００５９】

受信装置２の電子文書検証部１５は、受信装置２のデータベース１８を参照して、送信者認証子と送信装置１の公開鍵証明書とを照合し、送信者認証子が送信装置１の公開鍵証明書と一致するか否かを検証する（ステップＢ１１）。

検証の結果、一致するため、受信装置２の電子文書検証部１５は、送信装置１が第１電子文書を送信したことを認識する（ステップＢ１２）。

【００６０】

このように、本発明の電子データ送受信システムによれば、受信装置２が第６電子文書、第５電子文書、第４電子文書、第３電子文書、第２電子文書、第１電子文書の順で正しく確認（検証）できた場合、第１電子文書は、送信装置１によって送信されたことが保証される。また、本発明の電子データ送受信システムによれば、受信装置２は、署名の履歴として第１電子文書が受信装置２に送信された経路（送信装置１、受付機器５－１、中継器５－２、中継器５－３、中継器５－４、受付機器５－５、受信装置２）を検証することができる。受信者は、その経路をオフラインで確認することができる。この受信装置２は、受付機器５－１、中継器５－２、中継器５－３、中継器５－４、受付機器５－５と通信してログを収集することなく、第１電子文書が送信された経路をオフラインで確認することができる。このため、受付機器５－１、中継器５－２、中継器５－３、中継器５－４、受付機器５－５は、ログを格納する必要がなく、そのための記憶装置を必要としない。また、本発明の電子データ送受信システムは、受信装置２によって経路を把握するため、ハッカーを防止する。

【００６１】

次に、送信装置１が行う受信証拠データの検証について説明する。

【００６２】

図１２に示されるように、送信装置１の電子文書検証部１５は、送信装置１のデータベース１８を参照して、記憶装置３に格納された受信証拠データの署名と受付機器５－５の公開鍵証明書とを照合し、受信証拠データの署名が受付機器５

－５の公開鍵証明書と一致するか否かを検証する（ステップＣ１）。

検証の結果、一致するため、送信装置１の電子文書検証部１５は、受信証拠データに付与された受付機器５－５の署名を除いた第５電子文書と受信者認証子と第２タイムスタンプとを取出す（ステップＣ２、図１０参照）。

【００６３】

送信装置１の電子文書検証部１５は、送信装置１のデータベース１８を参照して、受信者認証子と受信装置２の公開鍵証明書とを照合し、受信者認証子が送信装置１の公開鍵証明書と一致するか否かを検証する（ステップＣ３）。

検証の結果、一致するため、送信装置１の電子文書検証部１５は、送信装置１のデータベース１８を参照して、第５電子文書の署名と中継機器５－４の公開鍵証明書とを照合し、第５電子文書の署名が中継機器５－４の公開鍵証明書と一致するか否かを検証する（ステップＣ４）。

検証の結果、一致するため、送信装置１の電子文書検証部１５は、第５電子文書に付与された中継機器５－４の署名を除いた第４電子文書を取出す（ステップＣ５、図１０参照）。

【００６４】

送信装置１の電子文書検証部１５は、送信装置１のデータベース１８を参照して、第４電子文書の署名と中継機器５－３の公開鍵証明書とを照合し、第４電子文書の署名が中継機器５－３の公開鍵証明書と一致するか否かを検証する（ステップＣ６）。

検証の結果、一致するため、送信装置１の電子文書検証部１５は、第４電子文書に付与された中継機器５－３の署名を除いた第３電子文書を取出す（ステップＣ７、図１０参照）。

【００６５】

送信装置１の電子文書検証部１５は、送信装置１のデータベース１８を参照して、第３電子文書の署名と中継機器５－２の公開鍵証明書とを照合し、第３電子文書の署名が中継機器５－２の公開鍵証明書と一致するか否かを検証する（ステップＣ８）。

検証の結果、一致するため、送信装置１の電子文書検証部１５は、第３電子文

書に付与された中継機器５－２の署名を除いた第２電子文書を取出す（ステップＣ９、図１０参照）。

【００６６】

送信装置１の電子文書検証部１５は、送信装置１のデータベース１８を参照して、第２電子文書の署名と受付機器５－１の公開鍵証明書とを照合し、第２電子文書の署名が受付機器５－１の公開鍵証明書と一致するか否かを検証する（ステップＣ１０）。

検証の結果、一致するため、送信装置１の電子文書検証部１５は、第２電子文書に付与された受付機器５－１の署名を除いた第１電子文書と送信者認証子と第１タイムスタンプとを取出す（ステップＣ１１、図１０参照）。

【００６７】

送信装置１の電子文書検証部１５は、記憶装置３を参照して、いま取出した第１電子文書と記憶装置３に格納されている保管用電子文書（第１電子文書）とを照合し、取出した第１電子文書が保管用電子文書と一致するか否かを検証する（ステップＣ１２）。

検証の結果、一致するため、送信装置１の電子文書検証部１５は、第１電子文書が改ざんされることなく受信装置２に送信されたことを認識する（ステップＣ１３）。

【００６８】

このように、本発明の電子データ送受信システムによれば、送信装置１が受信証拠データ、第５電子文書、第４電子文書、第３電子文書、第２電子文書、第１電子文書の順で正しく確認（検証）できた場合、第１電子文書は、受信装置２によって受信されたことが保証される。また、本発明の電子データ送受信システムによれば、送信装置１は、取出した第１電子文書と記憶装置３に格納されている保管用電子文書（第１電子文書）とを比較することで第１電子文書の改ざんを検出できる。本発明の電子データ送受信システムによれば、送信装置１は、署名の履歴として第１電子文書が受信装置２に送信された経路（送信装置１、受付機器５－１、中継器５－２、中継器５－３、中継器５－４、受付機器５－５、受信装置２）を検証することができる。送信者は、その経路をオフラインで確認するこ

とができる。この送信装置１は、受付機器５－１、中継器５－２、中継器５－３、中継器５－４、受付機器５－５と通信してログを収集することなく、第１電子文書が送信されてきた経路をオフラインで確認することができる。このため、受付機器５－１、中継器５－２、中継器５－３、中継器５－４、受付機器５－５は、ログを格納する必要がなく、そのための記憶装置を必要としない。また、本発明の電子データ送受信システムは、送信装置１によって経路を把握するため、ハッカーを防止する。

【００６９】

上述のステップＡ３６にて受信証拠データを生成する場合、電子文書は省略してもよい（図１４参照）。

【００７０】

この場合、図１３に示されるように、受付機器５－５の証拠データ生成部２５は、ステップＡ３６にて受信証拠データを生成した後、その受信証拠データから第１電子データを削除する（ステップＡ４０）。受付機器５－５の送信部２１は、ステップＡ３６にて、第１電子データが削除された受信証拠データを送信装置１に送信する。

送信装置１の受信部１２は、第１電子データが削除された受信証拠データを受付機器５－５から受信する。このとき、送信装置１の署名検証部１４は、第１電子データが削除された受信証拠データに、記憶装置３に格納されている保管用電子文書（第１電子文書）を付加して受信証拠データを復元する（ステップＡ４１）。その後、送信装置１は、ステップＡ３８、Ａ３９、Ｃ１～Ｃ１３を実行する。

【００７１】

【発明の効果】

本発明の電子データ送受信システムによれば、送受信装置１（送信装置１）が送信した電子データ（第１電子文書）を送受信装置２（受信装置２）が受信するまで保証する。

また、本発明の電子データ送受信システムによれば、送受信装置１（送信装置１）、送受信装置２（受信装置２）は、電子データ（第１電子文書）が送受信装

置２（受信装置２）に送信された経路を検証することができる。

また、本発明の電子データ送受信システムによれば、送受信装置１（送信装置１）は、電子データ（第１電子文書）と記憶装置３に格納されている電子データ（第１電子文書）とを比較することで改ざんを検出できる。

また、本発明の電子データ送受信システムによれば、送受信装置１（送信装置１）、送受信装置２（受信装置２）によって経路を把握するため、ハッカーを防止する。

【図面の簡単な説明】

【図１】

図１は、本発明の電子データ送受信システムの構成を示す図である。

【図２】

図２は、本発明の電子データ送受信システムの概念を示す図である。

【図３】

図３は、本発明の電子データ送受信システムの送受信装置の構成を示す図である。

【図４】

図４は、本発明の電子データ送受信システムの受付機器の構成を示す図である。

【図５】

図５は、本発明の電子データ送受信システムの中継機器の構成を示す図である。

【図６】

図６は、本発明の電子データ送受信システムの動作を示すフローチャートである。

【図７】

図７は、本発明の電子データ送受信システムの動作を示すフローチャートである。

【図８】

図８は、本発明の電子データ送受信システムの動作を示すフローチャートであ

る。

【図９】

図９は、本発明の電子データ送受信システムにおける電子文書を説明するための図である。

【図１０】

図１０は、本発明の電子データ送受信システムにおける電子文書を説明するための図である。

【図１１】

図１１は、本発明の電子データ送受信システムの動作を示すフローチャートである。

【図１２】

図１２は、本発明の電子データ送受信システムの動作を示すフローチャートである。

【図１３】

図１３は、本発明の電子データ送受信システムの動作を示すフローチャートである。

【図１４】

図１４は、本発明の電子データ送受信システムにおける電子文書を説明するための図である。

【符号の説明】

１　　送受信装置（送信装置）

２　　送受信装置（受信装置）

３、４　　記憶装置

５－１、５－５　　受付機器

５－２、５－３、５－４　　中継機器

１１、２１、３１　　送信部

１２、２２、３２　　受信部

１３、２３、３３　　署名部

１４、２４、３４　　署名検証部

１５　　電子文書検証部

１６　　電子文書作成部

１７　　登録部

１８、２８、３８　　データベース

２５　　証拠データ生成部

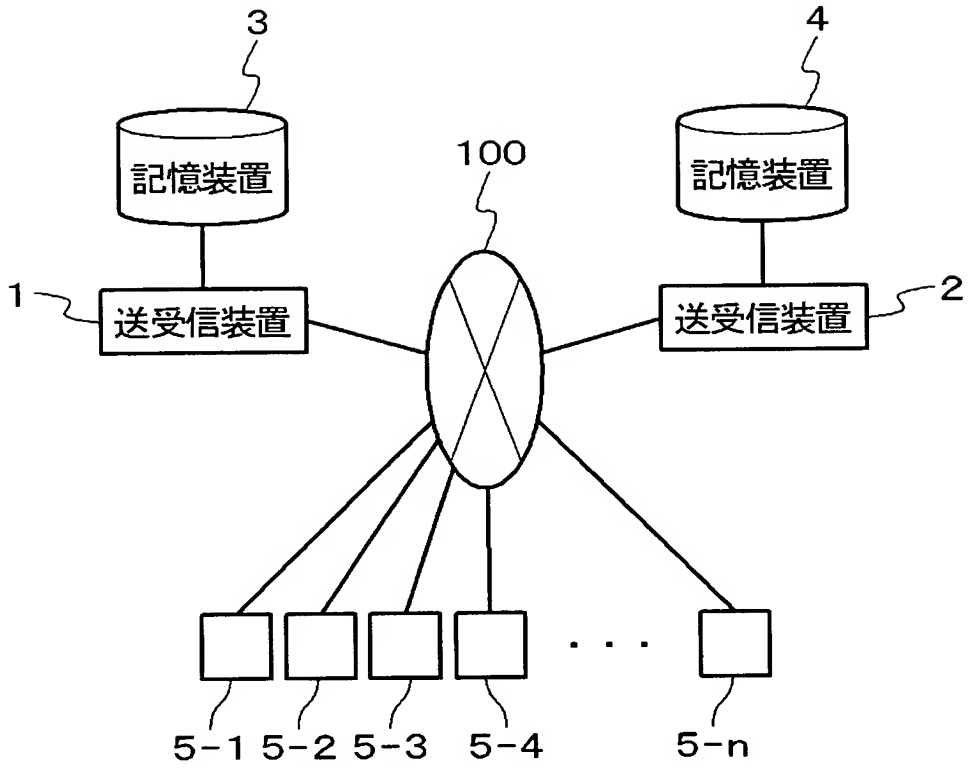
２６　　タイムスタンプ生成部

２７　　保存制御部

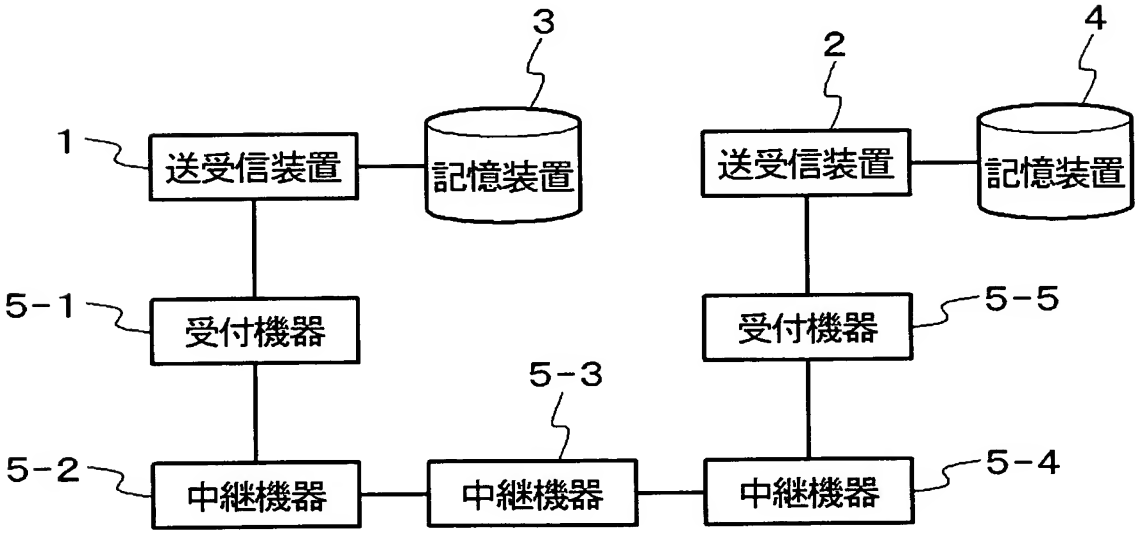
１００　　ネットワーク

【書類名】　図面

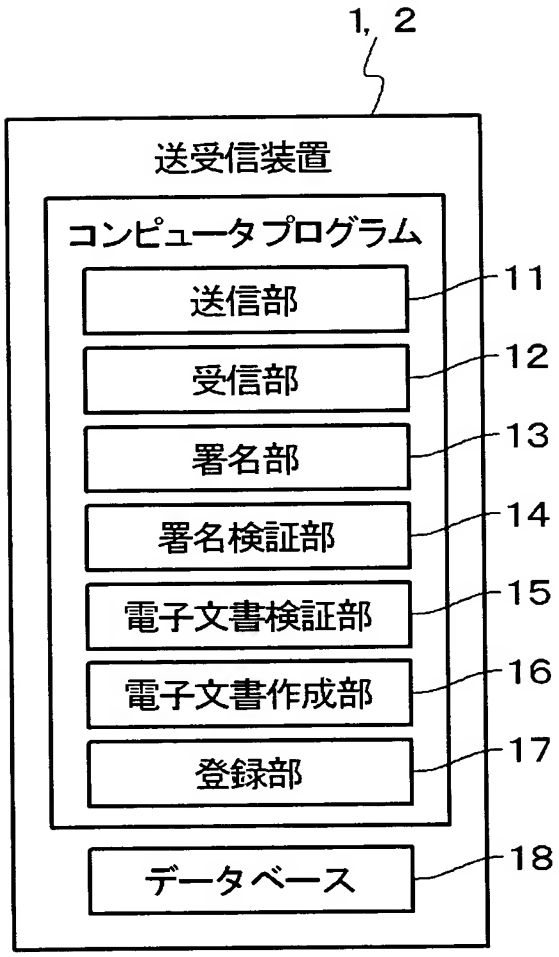
【図１】


3
4
記憶装置
100
記憶装置
1
送受信装置
送受信装置
2
5-1 5-2 5-3 5-4 5-n

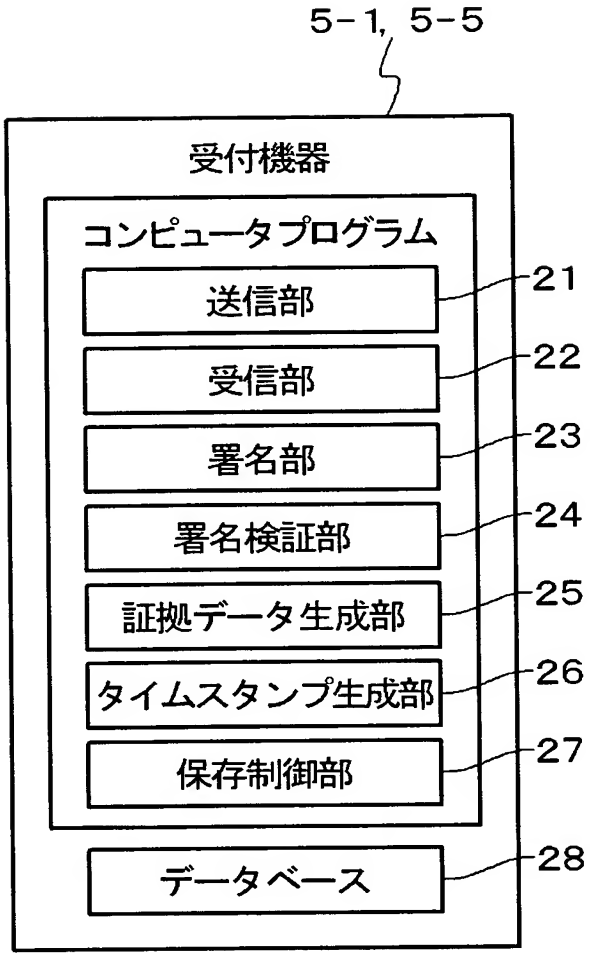
【図２】


3
2
4
1
送受信装置
記憶装置
送受信装置
記憶装置
5-1
受付機器
受付機器
5-5
5-3
5-2
中継機器
中継機器
中継機器
5-4

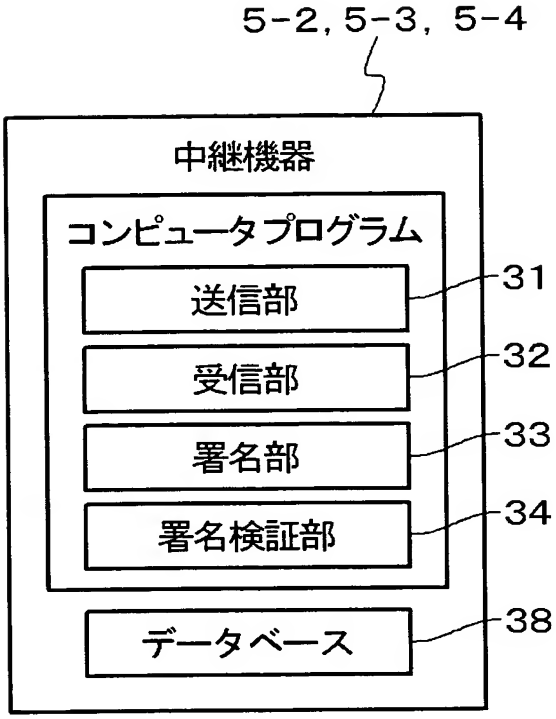
【図３】


1, 2
送受信装置
コンピュータプログラム
送信部
受信部
署名部
署名検証部
電子文書検証部
電子文書作成部
登録部
データベース
11
12
13
14
15
16
17
18

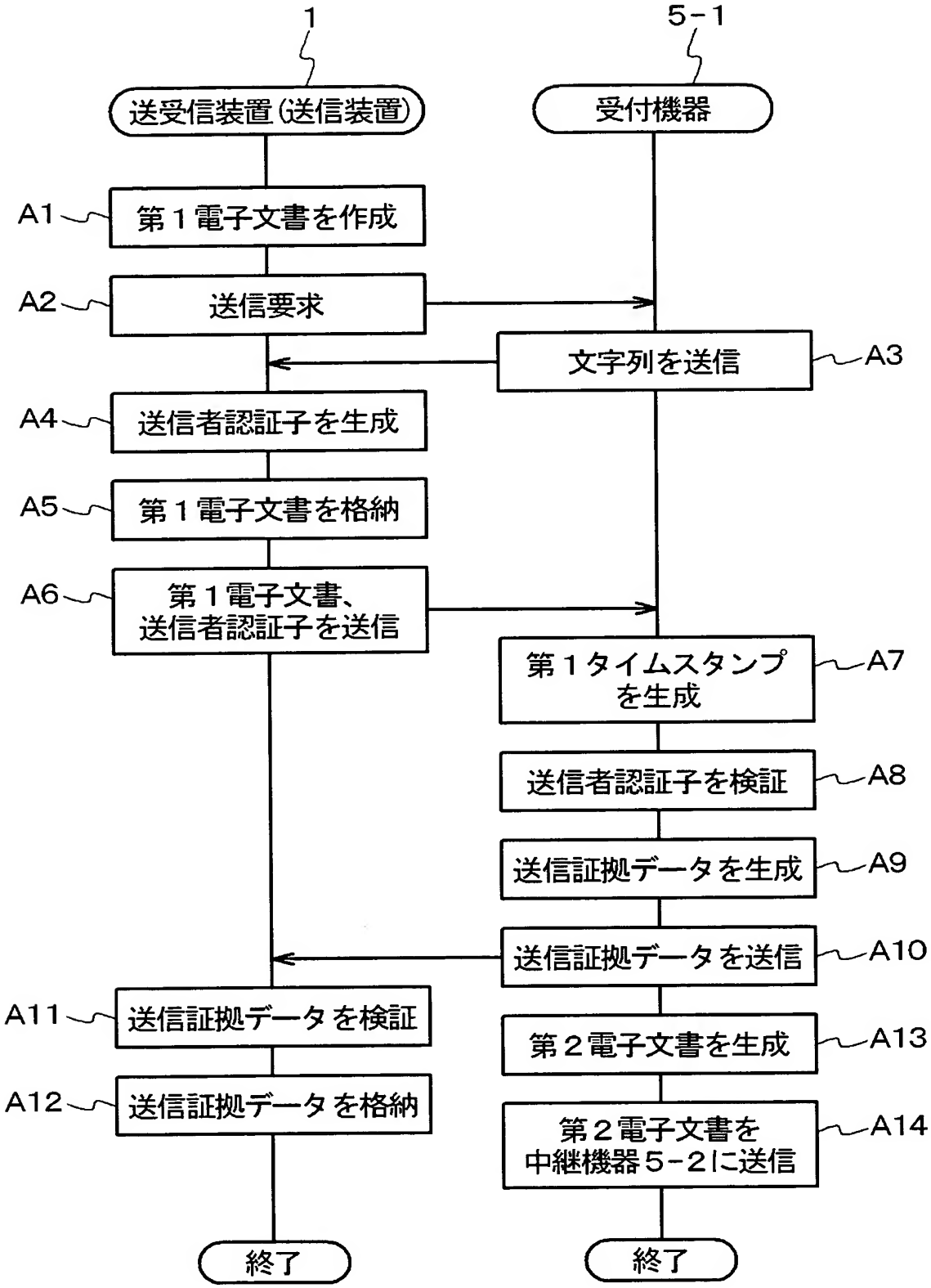
【図４】


5-1, 5-5
受付機器
コンピュータプログラム
送信部
21
受信部
22
署名部
23
署名検証部
24
証拠データ生成部
25
タイムスタンプ生成部
26
保存制御部
27
データベース
28

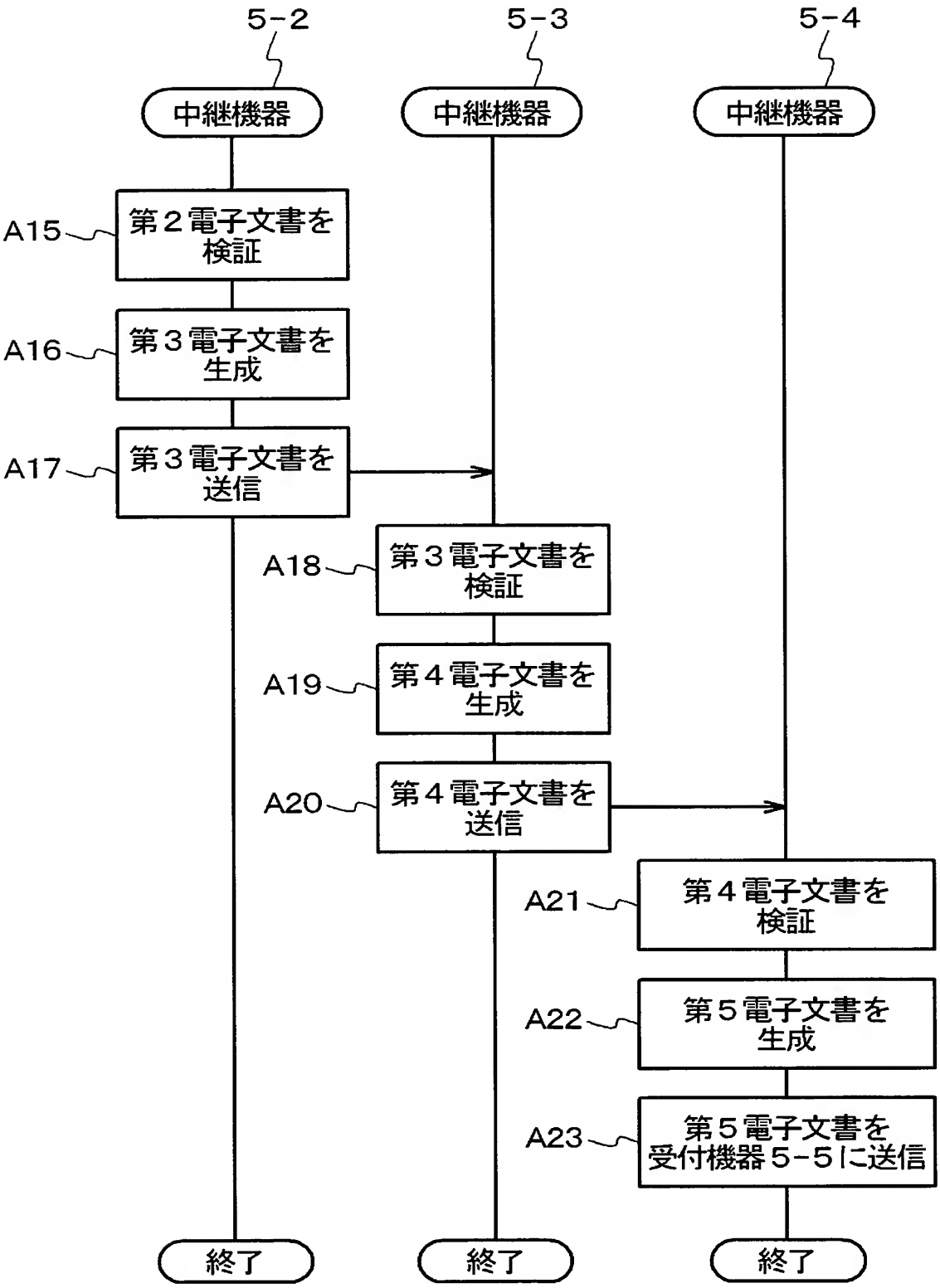
【図５】


5-2, 5-3, 5-4
中継機器
コンピュータプログラム
送信部
受信部
署名部
署名検証部
データベース
31
32
33
34
38

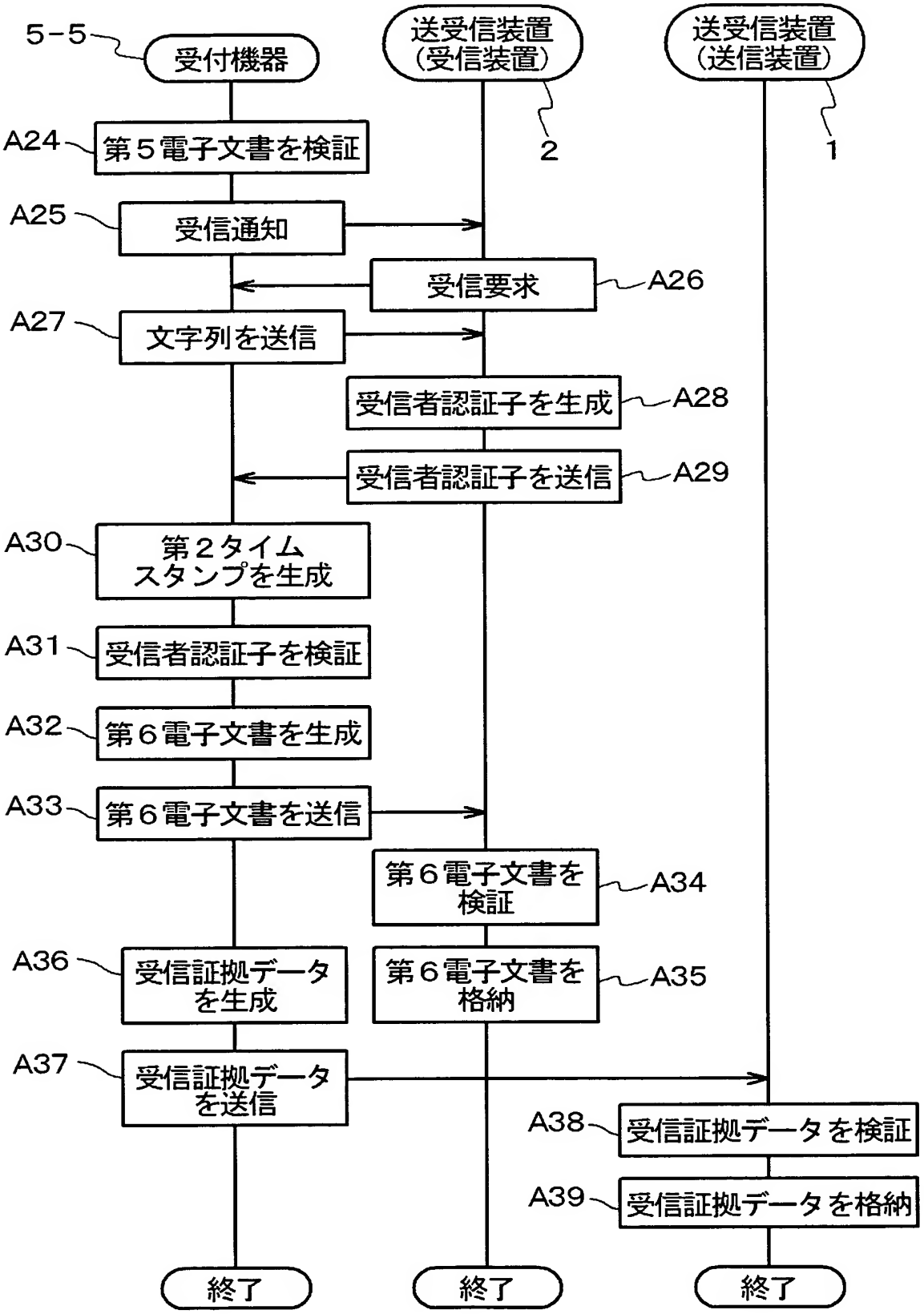
【図６】


1
5-1
送受信装置(送信装置)
受付機器
A1
第１電子文書を作成
A2
送信要求
文字列を送信
A3
A4
送信者認証子を生成
A5
第１電子文書を格納
A6
第１電子文書、
送信者認証子を送信
第１タイムスタンプ
を生成
A7
送信者認証子を検証
A8
送信証拠データを生成
A9
送信証拠データを送信
A10
A11
送信証拠データを検証
第２電子文書を生成
A13
A12
送信証拠データを格納
第２電子文書を
中継機器５-２に送信
A14
終了
終了

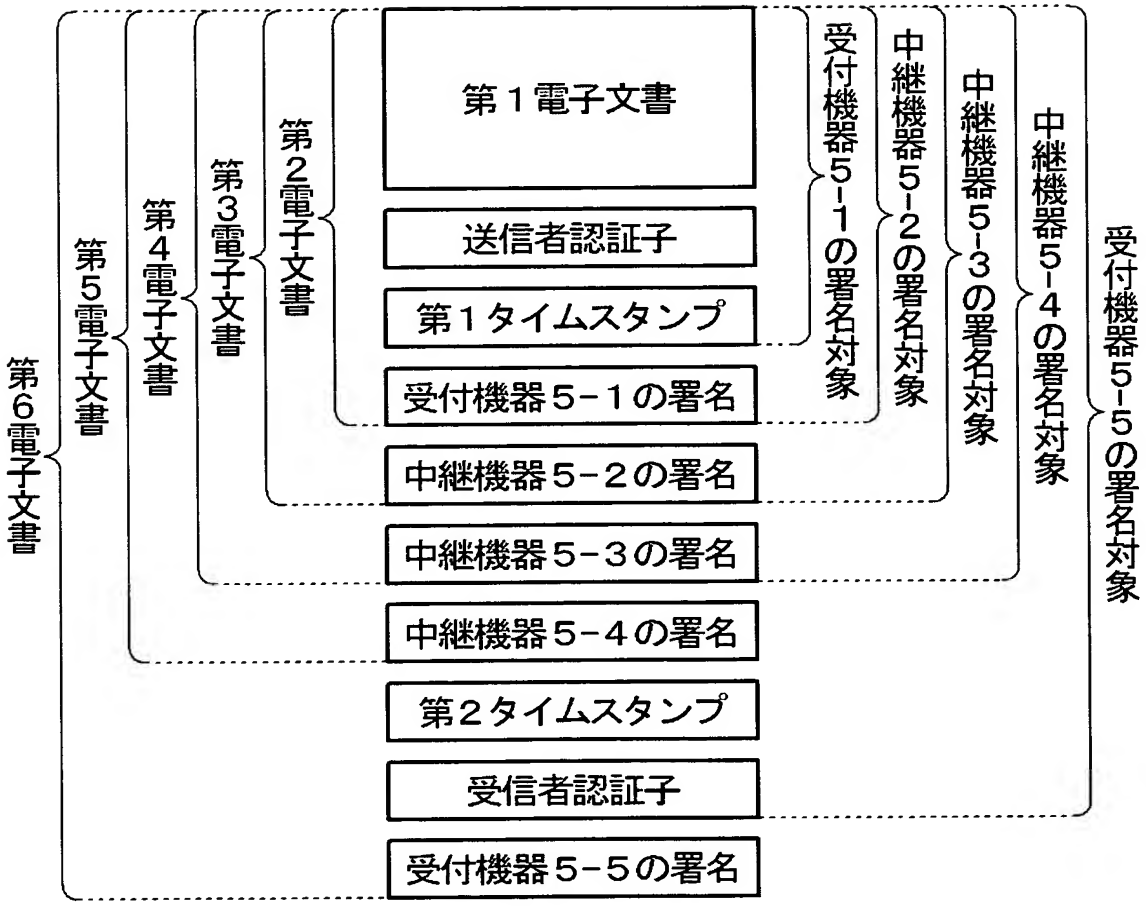
【図７】


5-2
5-3
5-4
中継機器
中継機器
中継機器
A15
第２電子文書を検証
A16
第３電子文書を生成
A17
第３電子文書を送信
A18
第３電子文書を検証
A19
第４電子文書を生成
A20
第４電子文書を送信
A21
第４電子文書を検証
A22
第５電子文書を生成
A23
第５電子文書を受付機器５-５に送信
終了
終了
終了

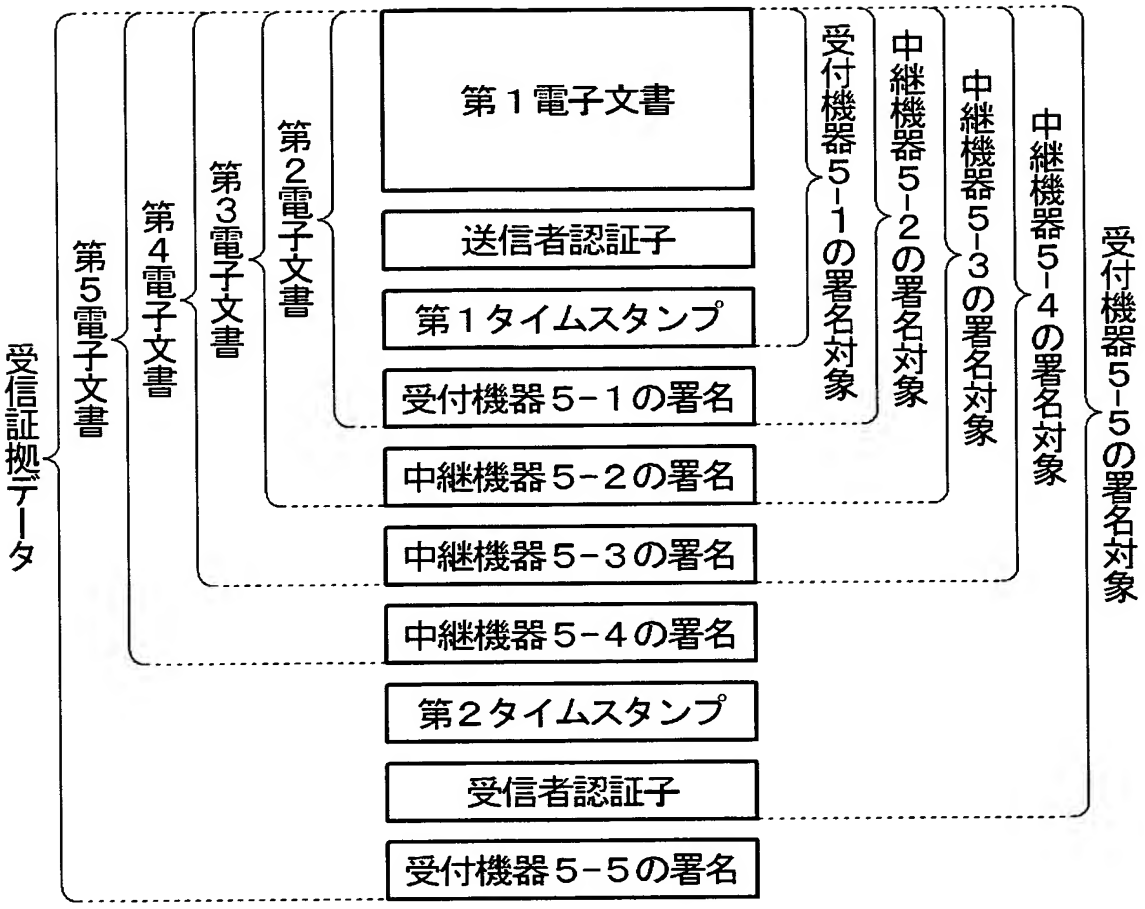
【図８】


5-5
受付機器
送受信装置
(受信装置)
2
送受信装置
(送信装置)
1
A24
第５電子文書を検証
A25
受信通知
受信要求
A26
A27
文字列を送信
受信者認証子を生成
A28
受信者認証子を送信
A29
A30
第２タイム
スタンプを生成
A31
受信者認証子を検証
A32
第６電子文書を生成
A33
第６電子文書を送信
第６電子文書を
検証
A34
A36
受信証拠データ
を生成
第６電子文書を
格納
A35
A37
受信証拠データ
を送信
A38
受信証拠データを検証
A39
受信証拠データを格納
終了
終了
終了

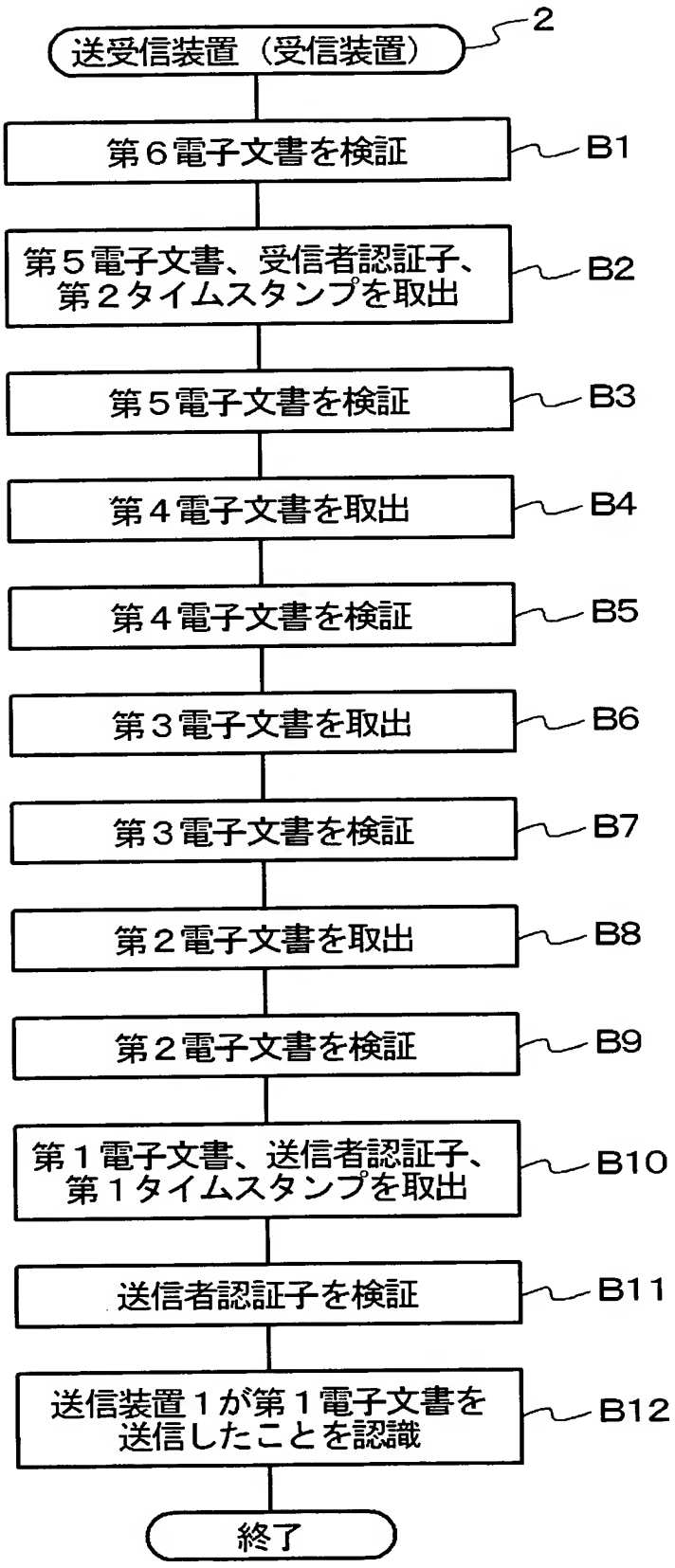
【図９】


第１電子文書
送信者認証子
第１タイムスタンプ
受付機器５－１の署名
中継機器５－２の署名
中継機器５－３の署名
中継機器５－４の署名
受信者認証子
受付機器５－５の署名
第２電子文書
第３電子文書
第４電子文書
第５電子文書
第６電子文書
受付機器５－１の署名対象
中継機器５－２の署名対象
中継機器５－３の署名対象
中継機器５－４の署名対象
受付機器５－５の署名対象

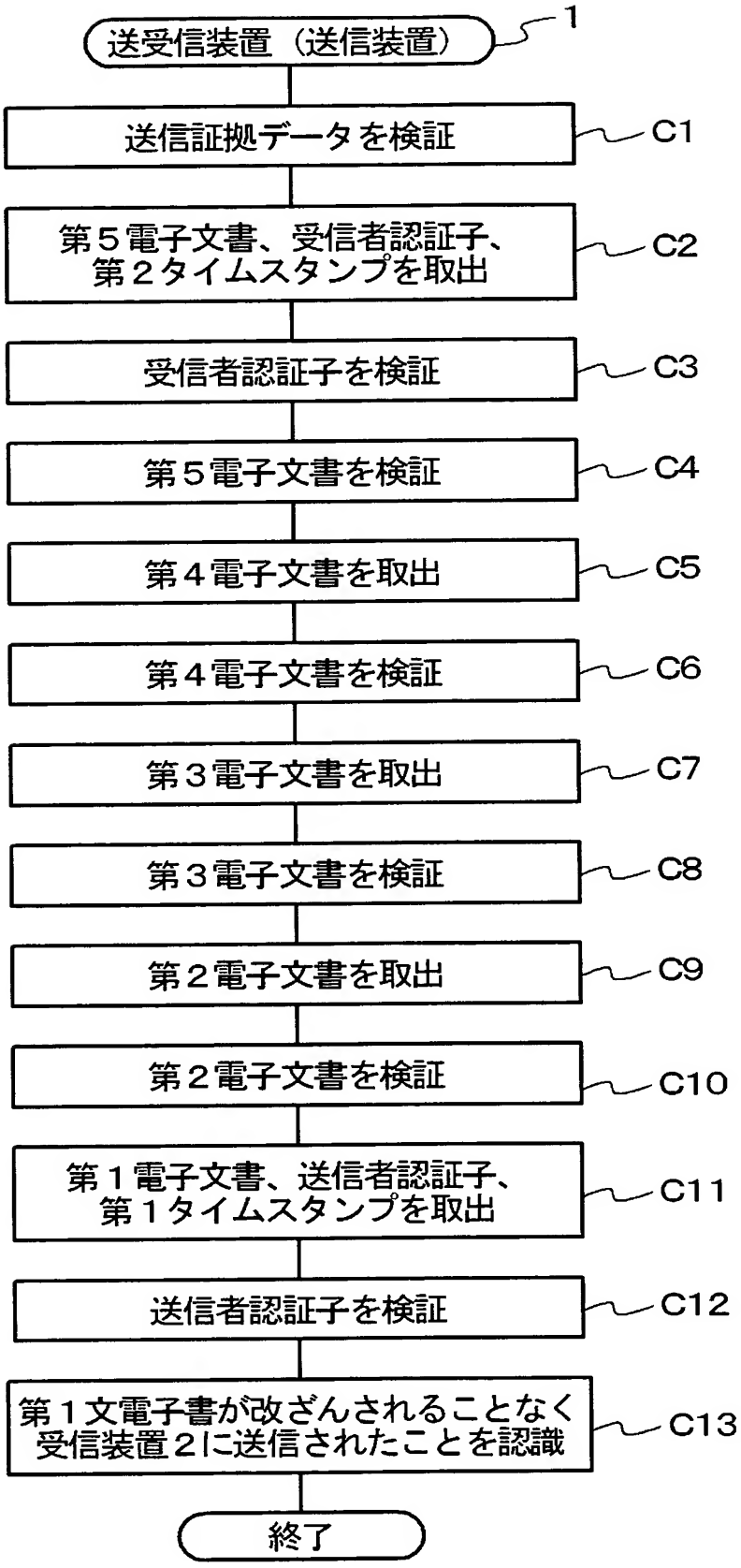
【図１０】


受信証拠データ
第５電子文書
第４電子文書
第３電子文書
第２電子文書
第１電子文書
送信者認証子
第１タイムスタンプ
受付機器５－１の署名
中継機器５－２の署名
中継機器５－３の署名
中継機器５－４の署名
第２タイムスタンプ
受信者認証子
受付機器５－５の署名
受付機器５－１の署名対象
中継機器５－２の署名対象
中継機器５－３の署名対象
中継機器５－４の署名対象
受付機器５－５の署名対象

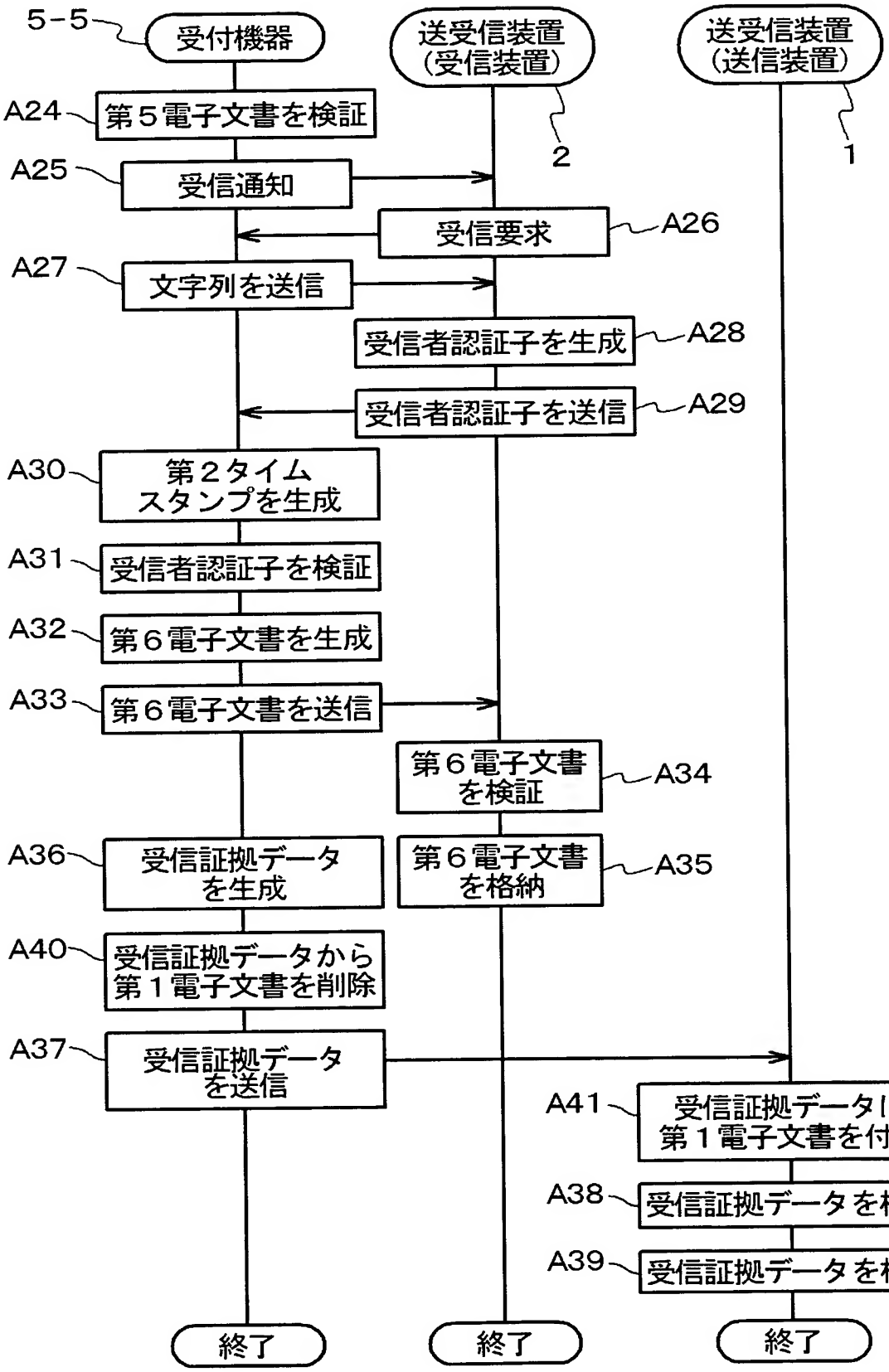
【図１１】


送受信装置（受信装置）
2
第６電子文書を検証
B1
第５電子文書、受信者認証子、第２タイムスタンプを取出
B2
第５電子文書を検証
B3
第４電子文書を取出
B4
第４電子文書を検証
B5
第３電子文書を取出
B6
第３電子文書を検証
B7
第２電子文書を取出
B8
第２電子文書を検証
B9
第１電子文書、送信者認証子、第１タイムスタンプを取出
B10
送信者認証子を検証
B11
送信装置１が第１電子文書を送信したことを認識
B12
終了

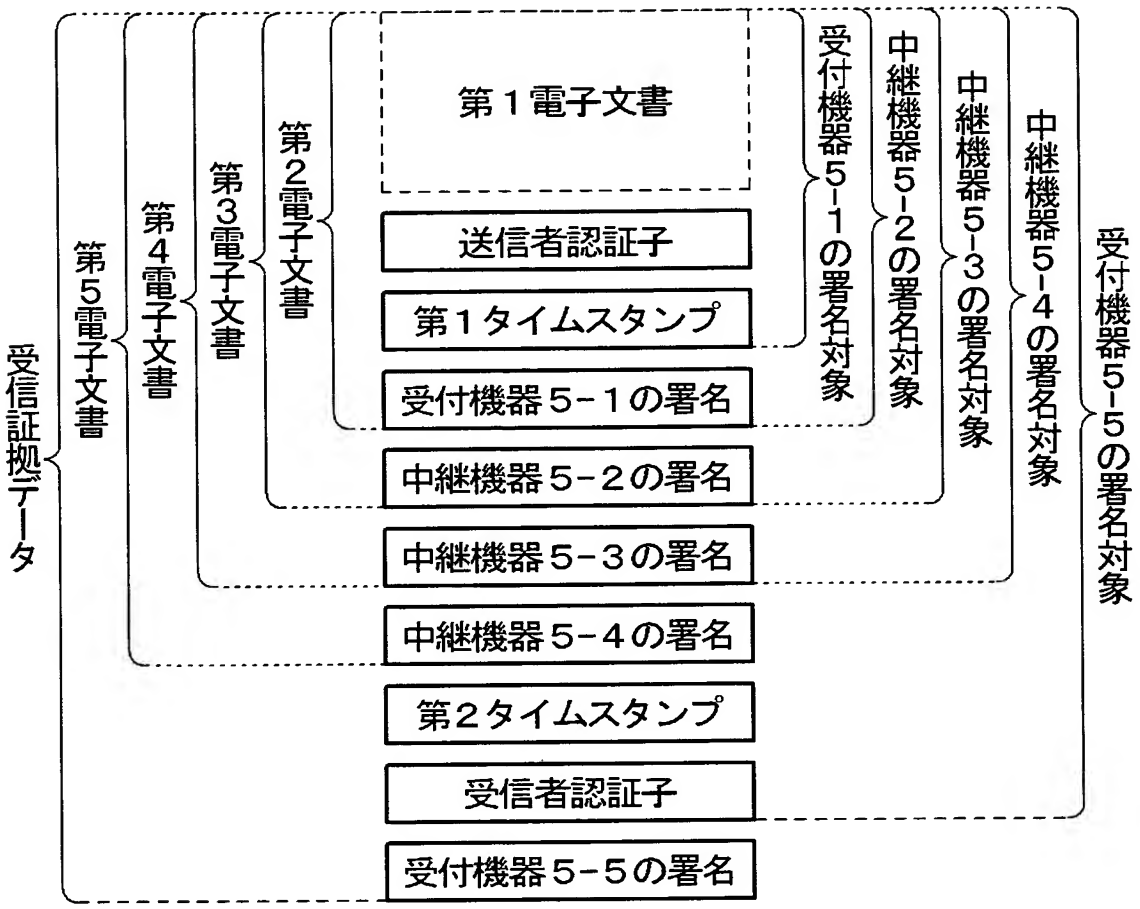
【図１２】


送受信装置（送信装置）
1
送信証拠データを検証
C1
第５電子文書、受信者認証子、
第２タイムスタンプを取出
C2
受信者認証子を検証
C3
第５電子文書を検証
C4
第４電子文書を取出
C5
第４電子文書を検証
C6
第３電子文書を取出
C7
第３電子文書を検証
C8
第２電子文書を取出
C9
第２電子文書を検証
C10
第１電子文書、送信者認証子、
第１タイムスタンプを取出
C11
送信者認証子を検証
C12
第１文電子書が改ざんされることなく
受信装置２に送信されたことを認識
C13
終了

【図１３】


5-5
受付機器
送受信装置
(受信装置)
2
送受信装置
(送信装置)
1
A24
第５電子文書を検証
A25
受信通知
受信要求
A26
A27
文字列を送信
受信者認証子を生成
A28
受信者認証子を送信
A29
A30
第２タイム
スタンプを生成
A31
受信者認証子を検証
A32
第６電子文書を生成
A33
第６電子文書を送信
第６電子文書
を検証
A34
A36
受信証拠データ
を生成
第６電子文書
を格納
A35
A40
受信証拠データから
第１電子文書を削除
A37
受信証拠データ
を送信
A41
受信証拠データに
第１電子文書を付加
A38
受信証拠データを検証
A39
受信証拠データを格納
終了
終了
終了

【図１４】


受信証拠データ
第５電子文書
第４電子文書
第３電子文書
第２電子文書
第１電子文書
送信者認証子
第１タイムスタンプ
受付機器５－１の署名
中継機器５－２の署名
中継機器５－３の署名
中継機器５－４の署名
第２タイムスタンプ
受信者認証子
受付機器５－５の署名
受付機器５－１の署名対象
中継機器５－２の署名対象
中継機器５－３の署名対象
中継機器５－４の署名対象
受付機器５－５の署名対象

【書類名】　要約書

【要約】

【課題】　送信装置が送信した電子データを受信装置が受信するまで保証する電子データ送受信システムを提供する。

【解決手段】　本発明の電子データ送受信システムは、ネットワーク［１００］に接続されたｎ個の装置［５－１～５－ｎ］と送信装置［１］と受信装置［２］とを具備する。送信装置［１］は、第１電子データを第１装置［５－１］に送信する。受信装置［２］は、第ｎ装置［５－ｎ］からの第（ｎ＋１）電子データを受信する。第ｊ装置（１≦ｊ≦ｎを満たす整数）は、自己を識別する署名を第ｊ電子データに付与した第（ｊ＋１）電子データを生成して第（ｊ＋１）装置に送信する。ここで、ｊがｎのとき、第（ｎ＋１）装置は受信装置［２］に対応する。本発明の電子データ送受信システムによれば、第（ｊ＋１）電子データが生成されるまでに付与された署名により、送信装置［１］が送信した第１電子データを受信装置［２］が受信するまで保証する。

【選択図】　図１

特願２００２－２９０３８７

出　願　人　履　歴　情　報

識別番号　　［０００００４２３７］

１．変更年月日　　１９９０年　８月２９日
［変更理由］　　新規登録
住　所　　東京都港区芝五丁目７番１号
氏　名　　日本電気株式会社